

January 16, 2001

M-01-08

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jack Lew
Director

SUBJECT: Guidance On Implementing the Government Information Security Reform Act

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform." It amends the Paperwork Reduction Act (PRA) of 1995 by enacting a new subchapter on "Information Security." The Act primarily addresses the program management and evaluation aspects of security. It covers unclassified and national security systems and creates the same management framework for each. At the policy level, the two types of systems remain separate. The Act became effective on November 29th and sunsets in two years.

The attachment provides guidance to agencies on carrying out the Act. The guidance focuses on unclassified Federal systems and addresses only those areas of the legislation that introduce new or modified requirements. The Act requires for both unclassified and national security programs: 1) annual agency program reviews; 2) annual Inspector General (IG) evaluations; 3) agency reporting to OMB the results of IG evaluations for unclassified systems and audits of IG evaluations for national security programs; and 4) an annual OMB report to Congress summarizing the materials received from agencies. Agencies will submit this information beginning in 2001 as part of the budget process.

The guidance also refers to some of the Act's provisions for national security systems. Unless otherwise specified, implementation of those provisions must be consistent with existing Presidential directives regarding national security systems.

This Act seeks to ensure proper management and security for the information resources supporting Federal operations and assets. It is particularly important as we move towards a more effective electronic government.

Please direct any questions about this guidance to Kamela White in the Office of Management and Budget at 202-395-3630, kgwhite@omb.eop.gov.

Attachment

**Guidance On Implementing the Government Information Security Reform Act
Title X, subtitle G of the 2001 Defense Authorization Act (P.L. 106-398)**

Part 1: General Overview

- A. How does the Security Act affect existing security policy and authorities?
- B. Does the Security Act pertain to existing agency systems?
- C. Does the Security Act pertain to contractor systems?
- D. How does the Security Act's new definition of "mission critical system" affect agency security responsibilities?
- E. What is the relationship between the new Security Act and PDD-63, "Critical Infrastructure Protection?"
- F. What are the relationships between the agency-wide security program and agency-wide security plan? Who is responsible for these and do individual systems still require security plans?

Part 2: Agency Responsibilities

- A. What new agency responsibilities are found in the Security Act?
- B. What are the responsibilities of the agency head?
- C. What are the responsibilities of program officials?
- D. What are the responsibilities of the agency Chief Information Officer?

Part 3: Inspector General Responsibilities

- A. What are the responsibilities of the agency Inspector General?

Part 4: OMB Responsibilities

- A. What are OMB's responsibilities under the Security Act?
- B. Will OMB be revising its security policies?

Part 5: Reporting Requirements

- A. What does the Security Act require agencies to report?
- B. What does the Security Act require OMB to report?

Part 6: Additional Responsibilities of Certain Agencies

- A. Department of Commerce
- B. Department of Defense and the Intelligence Community
- C. Department of Justice
- D. General Services Administration
- E. Office of Personnel Management

Part 1: General Overview

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform (The Security Act)." The Security Act was effective on November 29th and sunsets in two years.

The Security Act amends the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. Chapter 35), by enacting a new subchapter on "Information Security" which primarily addresses the program management and evaluation aspects of security. This Act applies to all agencies covered by the PRA. It covers programs for both unclassified and national security systems and within the agencies creates the same management framework for each. At the policy level, the two programs remain separate. The Security Act requires annual agency program reviews, annual Inspector General security evaluations, agency reporting to OMB, and an annual OMB report to Congress.

The following guidance focuses on unclassified Federal systems and addresses only those areas of the legislation that introduce new or modified requirements or that otherwise benefit from clarification. In several locations, this guidance refers to some of the Security Act's provisions for national security systems. Unless otherwise specified, implementation of those provisions will be consistent with existing Presidential directives regarding national security information and systems.

A. How does the Security Act affect existing security policy and authorities?

For unclassified systems, OMB retains its existing policy authority under the PRA and the Clinger-Cohen Act of 1996.

Except for the new annual program reviews, the role of the agency Inspector General, and the annual reporting requirement, the Security Act essentially codifies the existing requirements of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." The Security Act also requires agencies to incorporate security into the life cycle of agency information systems. For guidance on meeting this requirement, see OMB Memorandum 00-07, "Incorporating and Funding Security in Information Systems Investments," now incorporated into Section 8b(3) of OMB Circular A-130 (65 FR 77677; December 12, 2000). See, www.cio.gov/docs/Recompiled_A-1301.htm.

For national security systems, the Security Act directs OMB to delegate certain authorities to "the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President." The Security Act also directs OMB to delegate to the Secretary of Defense certain limited authorities concerning DOD unclassified mission critical systems. Delegations will be issued to appropriate agencies under separate cover, consistent with existing law and policy.

B. Does the Security Act pertain to existing agency systems?

Yes. The Security Act pertains to all systems supporting all operations and assets of an agency, including those systems currently in place or planned.

C. The Act states that DOD security policies also apply to DOD contractor systems. Do the security policies of other agencies also apply to their contractor's systems?

Yes. By using the Clinger-Cohen Act definition of information technology, the Security Act includes contractor systems. The Clinger-Cohen definition of information technology includes technology "used by the agency directly or is used by a contractor under contract to the agency. . ."

D. How does the Security Act's new definition of "mission critical system" affect agency security responsibilities?

The three-part definition for mission critical systems found in section 3532(b)(2) draws on the Computer Security Act of 1987 and the Clinger-Cohen Act. It is in the Security Act largely as a mechanism to keep separate the Security Act's requirements for policies concerning national security systems and unclassified systems. The Security Act reaffirms existing policy by requiring that agencies provide adequate security for all agency information, systems, operations, and assets.

The first part of the definition (section 3532(b)(2)(A)) references the Clinger-Cohen definition of national security systems. The second part (section 3532(b)(2)(B)) follows closely the Computer Security Act definition for systems processing national security information. The one change is that the word "secret" has been replaced by "classified" to reflect terminology used in Executive Order 12958, "Classified National Security Information." The Security Act combines these two types of systems for the purposes of establishing a policy framework that is separate and apart from the program for unclassified systems. Existing Presidential directives form the policy framework for securing national security systems. For the purposes of simplicity, this guidance refers to these systems as "national security systems."

The third part of the definition (section 3532(b)(2)(C)) is a modified Computer Security Act definition of systems processing sensitive, but unclassified, information.

By reiterating existing statutory definitions for national security systems and unclassified systems, the Security Act recognizes the distinctly different policy and oversight needs of the two programs and maintains the longstanding separation of the two.

E. What is the relationship between the new Security Act and PDD-63?, "Critical Infrastructure Protection?"

The Security Act compliments and does not conflict with PDD-63. Agencies should view their PDD-63 requirements in two ways. The first, especially for those agencies designated as lead agencies by the PDD, concerns interaction with industry: the new Security Act has no direct relationship to that role. The second concerns every agency's requirement to protect its critical infrastructures and, working with other agencies, to establish the Federal government as a model

for security. These PDD requirements and the new Security Act (as is true for existing law and security policy) are complementary and not conflicting.

For agency operations and assets (including systems) the critical infrastructure protection program is largely an identification and prioritization effort. Within this effort an agency identifies its enterprise architecture, interdependencies, and relationships. Thereafter, it is incumbent upon the agency to apply applicable security policies (for unclassified systems or national security systems) to protect their operations and assets adequately while understanding the shared risk environment in which they operate. Again, within the agency asset context, the major thrust of critical infrastructure protection should be to concentrate on and ensure the security of those assets that are most critical. Agencies must ensure that they integrate their security programs and critical infrastructure protection efforts. For additional information on enterprise architecture see Section 8b of OMB Circular A-130 (65 FR 77677; December 12, 2000).

The agency plans, programs, and reports required by the Security Act (discussed elsewhere in this guidance) should reflect the integration of the two programs within the agency and include as appropriate agency critical infrastructure protection efforts.

F. What are the relationships between the agency-wide security program and agency-wide security plan? Who is responsible for these and do individual systems still require security plans?

Agency Chief Information Officers (CIO) should develop, implement, and maintain an agency-wide security program and describe the program in detail in the agency-wide plan. The Security Act reemphasizes the CIO's strategic, agency-wide security responsibility.

Each agency program official should develop, implement, and maintain a security program (and document it in a plan) that assesses risk and provides adequate security for the operations and assets of programs and systems under their control. Each system requires a plan. Where appropriate, individual plans may be consolidated into one plan that reflects a logical grouping or collection of systems, provided that the security controls for each system are fully documented. In consultation with the agency CIO, program officials should ensure that their individual program and plan are consistent with and incorporated into the agency-wide security program and plan.

Part 2: Agency Responsibilities

The Security Act names specific authorities, responsibilities, and functions for the agency, the head of the agency, agency program officials, and the CIO of the agency.

A. What new agency responsibilities are found in the Security Act?

Agency responsibilities set forth in the Security Act remain largely the same as those required by existing law and policy. The following are those that are most noteworthy.

1. Agency-wide Program Practiced Throughout Life Cycle

Each agency will develop and implement an agency-wide risk-based security program to provide information security throughout the life cycle of all systems supporting their operations and assets. This continues requirements of existing law and policy that direct agencies to ensure that risk-based security is an integral part of the enterprise architecture and is included in the capital planning and investment control process.

2. Incident Response Capability

As found in existing policy, all agency programs will include procedures for detecting, reporting, and responding to security incidents, including notifying and consulting with law enforcement officials, other offices and authorities, and the General Services Administration's Federal Computer Incident Response Capability (FedCIRC).

The intent of the incident handling provision is to ensure that each agency has both the technical and procedural means in place to detect and appropriately report security incidents and share information on common vulnerabilities. Policies and procedures should be documented and remove unnecessary internal obstacles to the timely reporting to the appropriate authorities within the agency (for example, security officials and Inspectors General) and with external organizations (for example, FedCIRC, law enforcement e.g., the National Infrastructure Protection Center, and national security). Agencies should refer to the CIO Council's October 2000 memorandum regarding interaction with FedCIRC (www.cio.gov/docs/10_24FedCIRC_Note.htm). The Security Act directs the Department of Justice to develop guidance on such reporting to law enforcement.

In light of the Security Act's new role for agency Inspectors General, they must be an integral part of the reporting process.

For national security systems, the Security Act establishes a companion requirement for reporting incidents concerning national security systems. Implementation will be consistent with existing national security policy directives and will preserve existing agency authorities and the need-to-know principles regarding classified national security information.

3. Annual Program Review

Agency program officials, in consultation with the CIO, must review each agency-wide information security program at least annually. This annual review should also include reviews of all programs included in the agency-wide program. To promote consistent reviews across government, the CIO Council's Federal Information Technology Security Assessment Framework should form the basis for the annual program review. The National Institute of Standards and Technology will release in early 2001 a companion questionnaire to the Framework. See, www.cio.gov/docs/federal_it_security_assessment_framework.htm.

CIOs and program officials should coordinate their reviews with agency IGs to ensure consistent methodology and avoid unnecessary duplication of effort.

Agencies should report to OMB on their annual reviews when submitting their annual budget submissions, including an independent evaluation performed by the agency Inspector General.

4. Reporting Significant Deficiencies

Section 3534(c)(1)-(2) requires each agency to examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to: annual agency budgets; information resources management; performance and results based management under the Clinger-Cohen Act; program performance; and financial management.

The Security Act directs agencies to report findings of significant deficiencies in policy, procedures, or practice as a material weakness under the applicable criteria of other laws (see the Chief Financial Officers Act and the Federal Managers Financial Integrity Act). This provision does not establish new or expand existing criteria for determining material weaknesses within the requirements of those other laws. Rather, it establishes a logical relationship between agency security requirements and those other requirements. Thus, for example, the Federal Financial Management Improvement Act (FFMIA) and its implementing guidance does not recognize the concept of material weakness in computer security, as such, and therefore the findings from information security reviews would not necessarily need to be reported as separate findings under FFMIA (but would need to be taken into account in the analysis of financial systems performed under the Federal Managers' Financial Integrity Act.)

5. Annual Agency Performance Plan

Each agency, in consultation with the CIO, must include in their performance plan a description of the time periods for implementing the agency-wide security program that

is required under section 3534(d)(1), and the budget, staffing, and training resources which are necessary to implement this security program.

B. What are the responsibilities of the agency head?

Each agency must ensure the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems. Authenticity and nonrepudiation are security requirements addressed by the Government Paperwork Elimination Act and OMB Memorandum M-00-10, "OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act" (www.cio.gov/docs/m00-10.html).

Each agency must develop and implement information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of harm. The head of each agency must also ensure that the agency practices its information security program throughout the life cycle of each agency system. For guidance on accomplishing this requirement, see OMB Circular A-130 Section 8b(3) (65 FR 77677; December 12, 2000) on incorporating and funding security in information systems investments.

The agency head must submit annually to the Director of OMB the results of an independent evaluation performed by the agency Inspector General and, for national security systems, an audit of the independent review. This evaluation must accompany the agency's annual budget submission and should include the results of all annual program reviews by program officials.

C. What are the responsibilities of program officials?

Program officials must assess the risks to the operations and assets over which they have control. This includes determining the appropriate levels of security and periodically testing and evaluating security controls and techniques to ensure that they are cost effective and that they enable, but do not unnecessarily impede, business operations.

Each information security program under the Security Act, with the exception of national security programs, is subject to the approval of the Director of OMB. In addition, agency program officials in consultation with the agency CIO, must review each program at least annually. To promote consistent reviews and reporting across government, the agency's CIO should work with program officials in performing these reviews using the CIO Council's Federal Information Technology Security Assessment Framework as a basis for these program reviews.

These provisions continue the principle in existing OMB policy that agency program officials, not security officers or CIOs, are ultimately responsible for the security of programs under their control. This includes determining the acceptable level of risk and adequate level of security. It is essential that program officials work closely with CIOs and other officials to ensure a complete understanding of risks, especially the increased risks resulting from interconnecting with other programs and systems over which the program officials have little or no control.

D. What are the responsibilities of the agency Chief Information Officer?

The CIO must administer the agency functions under the Security Act. Consistent with the PRA and the Clinger-Cohen Act, this reconfirms the role of the CIO in providing a strategic view of the agency's architecture and crosscutting security needs.

The CIO should designate a senior agency information security official who will report to the CIO on the implementation and maintenance of the agency information security program and security policies. Most agencies have taken this action.

The CIO must participate in developing agency performance plans. These plans must include descriptions of the time periods required to implement the agency-wide security program required under section 3534(d)(1), and the budget, staffing, and training resources necessary to implement the program.

In fulfilling these requirements, agency CIOs must ensure that agency security programs integrate fully into the agency's enterprise architecture and capital planning and investment control processes. CIOs should work with agency program officials to ensure that the program officials understand and appropriately address risks, especially the increased risk resulting from interconnecting with other programs and systems over which the program officials have little or no control.

Part 3: Inspector General (IG) Responsibilities

A. What are the responsibilities of the agency IG?

IGs, or independent evaluators they choose, should perform an annual evaluation of the agency's security program and practices. This includes testing the effectiveness of security controls for "an appropriate subset of agency systems." Agencies without IGs should contract with an independent evaluator to perform the evaluation.

The appropriate subset provision reflects the realization that agencies cannot review all systems every year. Thus, IGs and other independent evaluators should identify and assess a logical representative sampling of systems that can be used to form the basis of a conclusion regarding the effectiveness of an agency's overall security program.

The IG or other independent evaluator may use any audit, evaluation, or report for the evaluation of agency programs or practices. This provision encourages IGs to use, to the extent practicable and weighing their quality, applicability and independence, those security program reviews, vulnerability assessments, audits, or evaluations performed by other experts. IGs should use results of the agency program reviews performed under the criteria of the CIO Council's Federal Information Technology Security Assessment Framework. Agency CIOs and program officials should work closely with agency IGs when developing their annual program review

methodology. Furthermore, the annual program reviews and IG evaluations called for under this new legislation should be closely coordinated with IG audits and evaluations already being performed pursuant to the Chief Financial Officers Act under criteria from the General Accounting Office.

This approach will help ensure that agencies perform adequate, independent reviews of their security programs while preserving scarce resources and avoiding unnecessary duplication of effort. Moreover, this approach will help IGs and agency program officials avoid unnecessarily competing for expert personnel and other resources.

For the first report due in September 2001 with the agency budget submission, IGs should use the requirements and criteria found in GAO's FISCAM, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," current NIST guidance, the CIO Council Framework, and information gleaned during their review of any agency security incidents that may have occurred at the agency during the evaluation period. Clearly, IGs may also use any other sources that they deem appropriate. Prior to the second annual report, OMB will reevaluate the scope as appropriate.

IGs should use a cutoff date for their evaluation period that permits reporting the evaluation with the agency's annual budget submission. For national security systems, agencies must submit to OMB copies of audits of the annual evaluations, also due with the agency's budget submission. Consistent with current practice, IGs may also submit copies of audits or evaluations directly to OMB.

Part 4: OMB Responsibilities

The Security Act codifies existing OMB policy, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources", and reiterates the requirements of the Computer Security Act of 1987, the PRA, and the Clinger-Cohen Act.

A. What are OMB's responsibilities under the Security Act?

Under the new Security Act, agency-wide security programs are subject to OMB "approval." OMB will implement this provision in a manner consistent with existing policy and practice. Generally, OMB approval will come from assessing performance through the agency self assessments, IG evaluations, and agency funding requests.

The Director of OMB has the authority to direct agencies to identify, use, and share best security practices; develop an agency-wide information security plan; incorporate information security principles and practices throughout the life cycles of the agency's information systems; and ensure that the agency's information security plan is practiced throughout the life cycles of the agency's information systems. Agencies should participate in the CIO Council's best security practices project to fulfill the first requirement.

The Director of OMB must submit to Congress an annual report that summarizes the program reviews and IG evaluations received from agencies.

In addition, the Director will establish government-wide policies for the management of programs that support cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations and include information technology architectures as defined under the Clinger-Cohen Act. Please see OMB Circular A-130 Section 8b(3) regarding incorporating and funding security in information systems investments.

B. Will OMB be revising its security policies?

Yes. Next spring OMB will begin revisions of OMB Circular A-130, Appendix III including conforming changes where necessary.

Part 5: Reporting Requirements

A. What does the Security Act require agencies to report?

The Security Act requires the agency head to report to OMB annually the results of each independent evaluation of the agency-wide information security program and practices of the agency. For national security systems, agencies are to provide the results of an audit of the evaluation.

Additionally, OMB will ask agencies to include the results of their annual program reviews also required by the Security Act and incorporate as appropriate reporting on their critical infrastructure protection efforts.

OMB will work with the agencies to develop a suitable form and format for agency reporting to OMB. Detailed guidance will be issued once a format is developed. It will ask agencies to submit their materials with their budget submissions.

B. What does the Security Act require OMB to report?

The Director of OMB will submit to Congress each year a report that summarizes the material received from agencies, including the annual IG evaluations, IG audits of evaluations of national security systems, and the program official's program reviews.

Part 6: Responsibilities of Certain Agencies

The Security Act charges the Department of Commerce, the Department of Defense and Intelligence Community, the Department of Justice, the General Services Administration, and the Office of Personnel Management with additional responsibilities.

A. Department of Commerce

The Department of Commerce (National Institute of Standards and Technology - NIST) retains its authorities and responsibilities as found in existing law and policy.

B. Department of Defense and the Intelligence Community

The Security Act directs the Secretary of Defense, the Director of Central Intelligence, and another agency head designated by the President to develop policies and guidelines for national security systems that are more stringent than those required for unclassified systems. This includes systems that are operated by the Department of Defense (DOD), a contractor of DOD, or another entity on behalf of DOD. The implementation of this provision will be consistent with existing Presidential directives concerning the protection of national security information and systems.

1. Under what circumstances can agencies apply the more stringent national security controls to unclassified systems?

The Security Act provides that more stringent policies and procedures may be adopted by OMB or other agencies to the extent that such policies are consistent with OMB policies and procedures. As with existing policy, agencies may employ more stringent controls when they have identified a compelling need to do so and can articulate that need.

The Security Act reinforces existing law and OMB policy that directs agencies to provide whatever levels of cost-effective, risk-based security that they deem necessary to mitigate the risks to their operations and assets. If an agency determines that national security policies and procedures are necessary for protecting an unclassified system, they may use them, provided that it articulates the basis for this decision. Agencies will not receive funding for the system unless they provide adequate justification. See OMB Circular A-130 Section 8b(3) regarding incorporating and funding security in information systems investments for additional guidance.

The Security Act does not provide authority to the Secretary of Defense or the Intelligence Community to establish or promote policies for unclassified systems not under their control.

C. Department of Justice

The Attorney General will review and update guidance to agencies on legal remedies regarding security incidents, on ways to report to and work with law enforcement agencies, and on lawful uses of security techniques and technologies.

This guidance should establish agreed upon thresholds for agency reporting of security incidents to law enforcement authorities and provide to the agencies acceptable uses of security controls such as intrusion detection and keystroke monitoring that maximize security while appropriately preserving the privacy of individuals. This guidance will reflect consultation with OMB and the agencies and will be consistent with OMB policies concerning security and privacy.

D. General Services Administration

The Security Act conveys authorities and responsibilities to the General Services Administration (GSA) that are today found in OMB policy and reflect the transfer of FedCIRC operations from NIST to GSA. These authorities include updating guidance on addressing security considerations when acquiring information technology, assisting agencies in fulfilling their incident handling requirements, and assisting agencies in the acquisition of cost-effective security products, services, and incident response capabilities. All such guidance must be consistent with and avoid unnecessary duplication of policy and guidance issued by OMB and NIST.

Beyond the authority to provide limited guidance described above, the Security Act does not provide any policy or guidance setting authority to GSA. From time-to-time, however, provided it is consistent with OMB policy and NIST guidance, GSA may issue operational procedures to assist agencies in improving the effectiveness of their incident handling capabilities. As has been the case with past practices, GSA will periodically report to OMB and NIST on findings, trends, and recommended remedies to causes of security incidents and vulnerabilities. OMB and NIST will use this information to inform the development of policy and guidance.

E. Office of Personnel Management

The Security Act conveys authorities and responsibilities to the Office of Personnel Management (OPM) that are today found in OMB policy. Additionally, it directs OPM to work with the National Science Foundation and other agencies on personnel and training initiatives for information security. Provided that adequate funds are appropriated, this language authorizes the establishment of a “Scholarship for Service” initiative and other Federal Cyber Services programs included in the President's FY 2001 budget.